

# **MULTIPLE TIERED NETWORK SECURITY SYSTEM, METHOD AND APPARATUS USING DYNAMIC USER POLICY ASSIGNMENT**

Inventors: Philip Kwan  
Chi-Jui Ho

## **BACKGROUND OF THE INVENTION**

### Field of the Invention

**[0001]** The present invention is generally directed to data communications networks. In particular, the present invention is directed to security features for controlling access to a data communications network.

### Background

**[0002]** There is an increasing demand for additional security features for controlling access to data communications networks. This is due, in large part, to an increase in the use of portable computing devices such as laptop computers and Voice Over Internet Protocol (VoIP) telephones, which can be easily moved from one point of network access to another. While such ease of access may be desirable from an end user perspective, it creates significant concerns from the perspective of network security.

**[0003]** For wired networks, recent security solutions from network vendors have involved pushing authentication functions out to the layer 2 port, such as to a layer 2 switch. One such solution involves authenticating the physical, or Media Access Control (MAC), address of a device coupled to the port of a layer 2 switch. Another solution involves enabling the switch to perform user authentication in accordance with protocols defined by the IEEE 802.1x standard. A further solution builds on the 802.1x protocol to dynamically assign an Access Control List ("ACL") or a MAC address filter to a port of a network switch based on the identity of a user. However, a majority of conventional switches do not provide the ability to implement all of these security features in a single network device.

[0004] A product marketed by Cisco Systems, Inc. of San Jose, California, designated the Catalyst 3550 Multilayer Switch, apparently provides a combination of the foregoing security features. However, the combination of physical (MAC) address authentication and 802.1x authentication is only provided in a multiple host ("multi-host") configuration, in which one or more computing devices are coupled to a single port of the switch via a central computing device. Furthermore, the 802.1x authentication is always performed prior to physical (MAC) address authentication in the Cisco product. Thus, when a computing device is coupled to a port of the Cisco switch, local resources (e.g., switch resources necessary to perform 802.1x authentication and, optionally, dynamic ACL and/or MAC address filter assignment) as well as network resources (e.g., communication between the switch and an authentication server) will always be expended to authenticate the user, prior to determining whether or not the physical (MAC) address of the device is valid. This results in a waste of such resources in the case where the device has an unauthorized MAC address.

[0005] What is needed then is a security solution that improves upon and addresses the shortcomings of known security solutions.

#### BRIEF SUMMARY OF THE INVENTION

[0006] The present invention is directed to a network security system, method and apparatus that substantially obviates one or more of the problems and disadvantages of the related art. In particular, the present invention is directed to a network access device, such as a network switch, that is used to implement a multiple key, multiple tiered system and method for controlling access to a data communications network in both a single host and multi-host environment. The system and method provide a first level of security that comprises authentication of the physical (MAC) address of a user device coupled to a port of the network access device, a second level of security that comprises authentication of a user of the user device if the first level of

security is passed, such as authentication in accordance with the IEEE 802.1x standard, and a third level of security that comprises dynamic assignment of a particular user policy to the port based on the identity of the user if the second level of security is passed, wherein access to the port is restricted in accordance with the user policy. The user policy may include an access control list (ACL) and/or a MAC address filter.

[0007] Co-pending and co-owned U.S. Patent Application Serial No. 10/458,628, entitled "Multiple Tiered Network Security System and Apparatus" to Kwan *et al.*, filed June 11, 2003, describes a network access device that implements a combination of security features including physical (MAC) address authentication, 802.1x user authentication, and dynamic virtual local area network (VLAN) assignment. As discussed in more detail in that application, which is incorporated by reference herein, dynamic VLAN assignment leverages the 802.1x user authentication protocol by dynamically assigning a port of a network access device to a predetermined VLAN based on user identification information provided pursuant to the protocol.

[0008] Dynamic VLAN assignment is very useful for small installations where complex VLANs are not in place. Installations that are configured to separate traffic of authenticated users into simple VLAN scenarios will find the dynamic VLAN assignment feature very useful. Examples of simple VLAN implementations may include: (1) VoIP VLAN vs. data VLAN; (2) Trusted User VLAN vs. Untrusted User VLAN; and (3) VLAN implementation where the same VLANs are implemented across all network access devices and each VLAN is uniformly defined to provide the identical levels of network access control.

[0009] However, for larger and more complex VLAN implementations that may spread across multiple countries or geographic areas, the definition of a VLAN may vary from each location or from network access device to network access device. In such cases, the dynamic VLAN assignment feature will not be very effective unless the VLANs are reconfigured. This may be very

difficult or even impossible to achieve depending on the complexity of the VLAN structure.

[0010] An embodiment of the present invention addresses this issue by utilizing dynamic user policies rather than, or in conjunction with, dynamic VLAN assignment to achieve granular, user-based network access control. A user policy may identify or include one or more access control lists (ACLs) and/or MAC address filters that restrict certain types of inbound and/or outbound traffic on a port. In accordance with an embodiment of the present invention, when a user is authenticated in accordance with the 802.1x protocol, an authentication server passes an accept message to a network access device that includes a user policy associated with the user. Based on this user policy, the network access device dynamically assigns the appropriate ACL(s) and/or MAC address filter(s) to the port to regulate network access.

[0011] In a further embodiment, the ACL(s) and/or MAC address filter(s) are dynamically assigned to the port provided that the sufficient system resources of the network access device can be allocated for this operation. If the system resources of the network access device are insufficient, then the port is blocked to the user—ie., the user remains unauthenticated by default.

[0012] The present invention provides improved network security as compared to conventional solutions, since it authenticates both the user device and the user. Moreover, the present invention provides network security in a manner more efficient than conventional solutions, since it performs physical (MAC) address authentication of a user device prior to performing the more resource-intensive step of performing user authentication, such as user authentication in accordance with a protocol defined by the IEEE 802.1x standard. Furthermore, the present invention provides granular, user-based network access control through the use of dynamic user policy assignment.

[0013] In accordance with one embodiment of the present invention, a network access device for providing network security is provided. The network access device includes a plurality of input ports and a switching fabric

for routing data received on the plurality of input ports to at least one output port. The network access device also includes control logic adapted to authenticate a physical address of a user device coupled to one of the plurality of input ports and to authenticate user information provided by a user of the user device only if the physical address is valid. Additionally, the control logic is adapted to restrict access to the particular input port in accordance with a user policy associated with the user information only if the user information is valid.

**[0014]** In an alternate embodiment of the present invention, a method for providing network security is provided. The method includes authenticating a physical address of a user device coupled to a port of a network access device, and authenticating user information provided by a user of the user device only if the physical address is valid. The method further includes restricting access to the port in accordance with a user policy associated with the user information only if the user information is valid.

**[0015]** In another embodiment of the present invention, a network system is provided. The system includes a data communications network, a network access device coupled to the data communications network, and a user device coupled to a port of the network access device. The network access device is adapted to authenticate a physical address of the user device and to authenticate user information provided by a user of the user device only if the physical address is valid. Additionally, the network access device is adapted to restrict access to the port in accordance with a user policy associated with the user information only if the user information is valid.

**[0016]** Further features and advantages of the invention, as well as the structure and operation of various embodiments of the invention, are described in detail below with reference to the accompanying drawings. It is noted that the invention is not limited to the specific embodiments described herein. Such embodiments are presented herein for illustrative purposes only. Additional embodiments will be apparent to persons skilled in the relevant art(s) based on the teachings contained herein.

## BRIEF DESCRIPTION OF THE DRAWINGS/FIGURES

- [0017] The accompanying drawings, which are incorporated herein and form part of the specification, illustrate the present invention and, together with the description, further serve to explain the principles of the invention and to enable a person skilled in the relevant art(s) to make and use the invention.
- [0018] FIG. 1 depicts the basic elements of a multiple tiered network security system implementing dynamic user policy assignment in accordance with an embodiment of the present invention.
- [0019] FIG. 2 depicts an exemplary high-level architecture of a network access device in accordance with an embodiment of the present invention.
- [0020] FIG. 3 illustrates a flowchart of a multiple tiered network security method that implements dynamic user policy assignment in accordance with an embodiment of the present invention.
- [0021] FIG. 4 illustrates a flowchart of a method for enabling physical address authentication of a network access device coupled to a data communications network in accordance with an embodiment of the present invention.
- [0022] FIG. 5 illustrates a flowchart of a method for performing user authentication and dynamic user policy assignment in accordance with an embodiment of the present invention.
- [0023] FIG. 6 depicts a multiple tiered network security system that accommodates a plurality of user devices in a multi-host configuration in accordance with an embodiment of the present invention.
- [0024] The features and advantages of the present invention will become more apparent from the detailed description set forth below when taken in conjunction with the drawings, in which like reference characters identify corresponding elements throughout. In the drawings, like reference numbers generally indicate identical, functionally similar, and/or structurally similar elements. The drawings in which an element first appears is indicated by the leftmost digit(s) in the corresponding reference number.

## DETAILED DESCRIPTION OF THE INVENTION

### A. Overview

[0025] The present invention is directed to a multiple key, multiple tiered network security system, method and apparatus. The system, method and apparatus provides at least three levels of security. The first level comprises physical MAC address authentication of a user device being attached to a network, such as a user device being coupled to a port of a network access device. The second level comprises authentication of the user of the user device, such as authentication in accordance with the IEEE 802.1x standard. The third level comprises dynamic assignment of a particular user policy to the port based on the identity of the user, wherein the user policy is used to selectively control access to the port. The user policy may identify or include an access control list (ACL) or MAC address filter. Failure to pass a lower security level results in a denial of access to subsequent levels of authentication.

### B. Multiple Tiered Security System, Method and Apparatus in Accordance with an Embodiment of the Present Invention

[0026] FIG. 1 depicts the basic elements of a multiple tiered network security system 100 in accordance with an embodiment of the present invention. As shown in FIG. 1, system 100 comprises a data communications network 104, a network access device 102 and an authentication server 106 each of which is communicatively coupled to data communications network 104, and a user device 108 communicatively coupled to network access device 102.

[0027] Data communications network 104 comprises a plurality of network nodes interconnected via a wired and/or wireless medium, wherein each node consists of a device capable of transmitting or receiving data over data communications network 104. In the embodiment described herein, data communications network 104 comprises a conventional local area network

("LAN") that employs an Ethernet communication protocol in accordance with the IEEE 802.3 standard for data link and physical layer functions. However, the invention is not so limited, and data communications network 104 may comprise other types of wired or wireless networks, including but not limited to a wide area network ("WAN"), and other types of communication protocols, including but not limited to ATM, token ring, ARCNET, or FDDI (Fiber Distributed Data Interface) protocols.

[0028] Network access device 102, which preferably comprises a network switch, comprises a plurality of ports for communicatively interconnecting network devices to each other and to data communications network 104. Network access device 102 is configured to channel data units, such as data packets or frames, between any two devices that are attached to it up to its maximum number of ports. In terms of the International Standards Organization's Open Systems Interconnection (OSI) model, network access device 102 performs layer 2, or data link layer, functions. In particular, network access device 102 examines each received data unit and, based on a destination address included therein, determines which network device the data unit is intended for and switches it out toward that device. In the embodiment described herein, the destination address comprises a physical or Media Access Control (MAC) address of a destination device.

[0029] FIG. 2 depicts an exemplary high-level architecture of network access device 102 in accordance with an embodiment of the present invention. As shown in FIG 2, network access device 102 comprises a plurality of input ports, 204a through 204n, that are coupled to a plurality of output ports, 206a through 206n, via a switching fabric 202. Network access device 102 also includes control logic 208 for controlling various aspects of switch operation and a user interface 210 to facilitate communication with control logic 208. User interface 210 provides a means for a user, such as a system administrator, to reconfigure network access device 102 and adjust operating parameters.

[0030] In operation, data units (e.g., packets or frames) are received and optionally buffered on one or more of input ports 204a through 204n. Control



logic 208 schedules the serving of data units received by input ports 204a through 204n in accordance with a predetermined scheduling algorithm. Data units are then served to switching fabric 202, which routes them to the appropriate output port 206a through 206n based on, for example, the destination address of the data unit. Output ports 206a through 206n receive and optionally buffer data units from switching fabric 202, and then transmit them on to a destination device. In accordance with an embodiment of the present invention, network access device 102 may also include logic for performing routing functions (layer 3 or network layer functions in OSI).

[0031] With further reference to FIG. 1, a user device 108 is shown connected to one of the ports of network access device 102. User device 108 may comprise a personal computer (PC), laptop computer, Voice Over Internet Protocol (VOIP) phone, a wireless access point, or any other device capable of transmitting or receiving data over a data communications network, such as data communications network 104. As described in more detail herein, the security features of the present invention are particularly useful in the instance where user device 108 is highly portable, and thus may be readily moved from one point of network access to another.

[0032] Authentication server 106 comprises a computer that stores application software and a database of profile information for performing a user authentication protocol that will be described in more detail herein. In an embodiment, authentication server 106 comprises a server that uses the Remote Authentication Dial-In User Service (RADIUS) as set forth in Internet Engineering Task Force (IETF) Request For Comments (RFC) 2865 for performing user authentication functions.

[0033] FIG. 3 illustrates a flowchart 300 of a multiple tiered network security method in accordance with an embodiment of the present invention. The invention, however, is not limited to the description provided by the flowchart 300. Rather, it will be apparent to persons skilled in the relevant art(s) from the teachings provided herein that other functional flows are within the scope and spirit of the present invention. Flowchart 300 will be described with

continued reference to example system 100 described above in reference to FIG. 1. The invention, however, is not limited to that embodiment.

[0034] The method of flowchart 300 begins at step 302, in which user device 108 is coupled to a port of network access device 102. Coupling user device 108 to a port of network access device 102 may comprise, for example, coupling user device 108 to an RJ-45 connector, which is in turn wired to a port of network access device 102.

[0035] At step 304, network access device 102 performs a physical (MAC) address authentication of user device 108. As will be described in more detail herein, network access device 102 performs this step by comparing a MAC address of user device 108 with a limited number of "secure" MAC addresses that are stored by network access device 102. As shown at step 306, if packets received from user device 108 have a source MAC address that does not match any of the secure addresses, then the protocol proceeds to step 308, in which network access device 102 either drops the packets or, alternately, disables the port entirely, thereby terminating the security protocol. In a further embodiment of the present invention, network access device 102 can also re-direct the packets to a network destination other than their originally intended destination based on the detection of an invalid source MAC address.

[0036] As further shown at step 306, if packets received from user device 108 have a source MAC address that does match one of the secure addresses, then the MAC address is valid and the security protocol proceeds to step 310.

[0037] At step 310, network access device 102 authenticates a user of user device 108 based upon credentials provided by the user. In an embodiment discussed in more detail herein, this step entails performing user authentication in accordance with the IEEE 802.1x standard, and involves sending the user credentials in a request message to authentication server 106 and receiving an accept or reject message in return, the accept or reject message indicating whether the user is valid. As shown at step 312, if the user is not valid, then the security protocol proceeds to step 314, in which network access device 102 blocks all traffic on the port except for the reception or

transmission of packets related to the user authentication protocol (e.g., 802.1x control packets). However, as also shown at step 312, if the user is valid, then the security protocol proceeds to step 316.

[0038] At step 316, network access device 102 determines whether a user policy has been provided for the user. As will be discussed in more detail herein, this step entails determining whether a user policy has been provided as part of the accept message returned from authentication server 106. A user policy may identify or include one or more access control lists (ACLs) or MAC address filters for controlling network access by the user. If a user policy has not been provided for the user, then no user policy is assigned to the port to which user device 108 is coupled as shown at step 318.

[0039] If, however, a user policy has been provided, then network access device 102 determines whether sufficient system resources are available to dynamically assign the user policy to the port, as shown at step 320. If sufficient resources are not available, then network access device 102 blocks all traffic on the port except for the reception or transmission of packets related to the user authentication protocol (e.g., 802.1x control packets) as shown at step 322. If sufficient resources are available, then network access device 102 dynamically assigns the user policy to the port and restricts traffic on the port in accordance with the policy, as shown at step 324.

[0040] With reference to the exemplary embodiment of FIG. 2, the security functions performed by network access device 102, as described above, are performed by control logic 208. As will be appreciated by persons skilled in the relevant art(s), such functions may be implemented in hardware, software or a combination thereof.

#### C. Physical Address Authentication of User Device in Accordance with an Embodiment of the Present Invention

[0041] As discussed above, network access device 102 is adapted to perform a physical (MAC) address authentication of a user device that is coupled to one of its ports. In particular, network access device 102 is adapted to store a

limited number of “secure” MAC addresses for each port. A port will forward only packets with source MAC addresses that match its secure addresses. In an embodiment, the secure MAC addresses are specified manually by a system administrator. In an alternate embodiment, network access device 102 learns the secure MAC addresses automatically. If a port receives a packet having a source MAC address that is different from any of the secure learned addresses, a security violation occurs.

[0042] With reference to the embodiment of network access device 102 depicted in FIG. 2, secure addresses for each input port 204a through 204n are stored in a local memory assigned to each port. Alternately, secure addresses are stored in a shared global memory, or in a combination of local and global memory.

[0043] In an embodiment, when a security violation occurs, network access device 102 generates an entry to a system log and an SNMP (Simple Network Management Protocol) trap. In addition, network access device 102 takes one of two actions as configured by a system administrator: it either drops packets from the violating address or disables the port altogether for a specified amount of time.

[0044] In a further embodiment of the present invention, a system administrator can configure network access device 102 to re-direct packets received from the violating address to a different network destination than that originally intended. Network access device 102 may achieve this by altering the packet headers. For example, network access device 102 may alter a destination address of the packet headers. Alternately, the re-direction may be achieved by generating new packets with identical data payloads but having different packet headers. As will be appreciated by persons skilled in the relevant art(s), the decision to configure network access device 102 to re-direct traffic from a violating address may be premised on the resulting burden to network access device 102 in handling traffic from that address.

[0045] FIG. 4 illustrates a flowchart 400 of a method for enabling physical address authentication of a device coupled to a data communications network

in accordance with an embodiment of the present invention. In particular, flowchart 400 represents steps performed by a system administrator in order to configure a network access device to perform physical address authentication in accordance with an embodiment of the invention. The invention, however, is not limited to the description provided by the flowchart 400. Rather, it will be apparent to persons skilled in the relevant art(s) from the teachings provided herein that other functional flows are within the scope and spirit of the present invention.

[0046] At step 402, the system administrator enables the MAC address authentication feature for one or more ports of the network access device. In an embodiment, the security feature is disabled on all ports by default, and a system administrator can enable or disable the feature globally on all ports at once or on individual ports.

[0047] At step 404, the system administrator sets a maximum number of secure MAC addresses for a port. In an embodiment, the network access device utilizes a concept of local and global “resources” to determine how many MAC addresses can be secured on each port. In this context, “resource” refers to the ability to store one secure MAC address entry. For example, each interface may be allocated 64 local resources and additional global resources may be shared among all the interfaces on the network access device.

[0048] In an embodiment, when the MAC address authentication feature is enabled for a port, the port can store one secure MAC address by default. A system administrator can then increase the number of MAC addresses that can be secured to a maximum of 64, plus the total number of global resources available. The number of addresses can be set to a number from 0 to (64 + the total number of global resources available). For example, the total number of global resources may be 2048 or 4096, depending on the size of the memory allocated. When a port has secured enough MAC addresses to reach its limit for local resources, it can secure additional MAC addresses by using global resources. Global resources are shared among all the ports on a first come, first-served basis.

**[0049]** At step 406, the system administrator sets an age timer for the MAC address authentication feature. In an embodiment, secure MAC addresses are not flushed when a port is disabled and brought up again. Rather, based on how the network access device is configured by the system administrator, the secure addresses can be kept secure permanently, or can be configured to age out, at which time they are no longer secure. For example, in an embodiment, the stored MAC addresses stay secure indefinitely by default, and the system administrator can optionally configure the device to age out secure MAC addresses after a specified amount of time.

**[0050]** At step 408, the system administrator specifies secure MAC addresses for a port. Alternately, the network access device can be configured to automatically “learn” secure MAC addresses by storing the MAC addresses of devices coupled to the port up to the maximum number of secure addresses for the port. These stored MAC addresses are then used as the secure addresses for authentication purposes.

**[0051]** At step 410, the system administrator optionally configures the network access device to automatically save the list of secure MAC addresses to a startup-configuration (“startup-config”) file at specified intervals, thus allowing addresses to be kept secure across system restarts. For example, learned secure MAC addresses can be automatically saved every twenty minutes. The startup-config file is stored in a memory within the network access device. In an embodiment, by default, secure MAC addresses are not automatically saved to a startup-config file.

**[0052]** At step 412, the system administrator specifies the action taken when a security violation occurs. In the case where the system administrator has specified the secure MAC addresses for the port, a security violation occurs when the port receives a packet with a source MAC address that is different than any of the secure MAC addresses. In the case where the port is configured to “learn” secure MAC addresses, a security violation occurs when the maximum number of secure MAC addresses has already been reached, and the port receives a packet with a source MAC address that is different than any

of the secure MAC addresses. In an embodiment, the system administrator configures the network access device to take one of two actions when a security violation occurs: either drop packets from the violating address or disable the port altogether for a specified amount of time.

D. User Authentication and Dynamic User Policy Assignment in Accordance with an Embodiment of the Present Invention

[0053] As discussed above, network access device 102 is further adapted to perform user authentication if user device 108 has a valid physical (MAC) address. In an embodiment, user authentication is performed in accordance with the IEEE 802.1x standard. As will be appreciated by persons skilled in the relevant art(s), the 802.1x standard utilizes the Extensible Authentication Protocol (EAP) for message exchange during the authentication process.

[0054] In accordance with 802.1x, a user (known as the supplicant) requests access to a network access point (known as the authenticator). The access point forces the user's client software into an unauthorized state that allows the client to send only an EAP start message. The access point returns an EAP message requesting the user's identity. The client returns the identity, which is then forwarded by the access point to an authentication server, which uses an algorithm to authenticate the user and then returns an accept or reject message back to the access point. Assuming an accept message was received, the access point changes the client's state to authorized and normal communication can take place.

[0055] In accordance with the embodiment of the invention described in reference to FIG. 1, and with reference to the 802.1x protocol described above, the user of user device 108 is the supplicant, network access device 102 is the authenticator, and authentication server 106 is the authentication server. In an embodiment, authentication server 106 comprises a server that uses the Remote Authentication Dial-In User Service (RADIUS) as described in RFC 2865, and may therefore be referred to as a RADIUS server.

**[0056]** In further accordance with an embodiment of the present invention, authentication server 106 provides a user policy to network access device 102 as part of the message granting authorization to a particular user. The user policy is included in an access profile for the user, which is configured by a network administrator and maintained in a database by authentication server 106. By storing the user policies on the authentication server, the policies only need to be created once—on the authentication server. When a user policy is passed back to network access device 102, network access device 102 determines if the user policy is valid, and, if so, dynamically assigns the user policy to the port to which user device 108 is coupled. In accordance with an embodiment of the present invention, a user policy may identify or include one or more access control lists (ACLs) or MAC address filters for controlling network access by the user.

**[0057]** An ACL is used to selectively permit or deny packets on a port in the inbound and/or outbound direction. An ACL filters traffic based on certain predefined criteria, and then either permits or denies traffic. As used herein, a “standard IP ACL” refers to an ACL that is used to permit or deny packets based on a source IP address of the packet. As also used herein, an “extended IP ACL” refers to an ACL that is used to permit or deny packets based on a source IP address, destination IP addresses, type of service, precedence, and/or protocol contained in the packet. TCP and UDP packets can be further filtered in accordance with an extended IP ACL by source and destination service ports. In accordance with an embodiment of the present invention, one IP ACL can be configured per port in the inbound direction and one IP ACL can be configured per port in the outbound direction. However, the invention is not so limited and, in an alternate embodiment, multiple ACLs may be configured per port in the inbound and/or outbound direction.

**[0058]** A MAC address filter is used to selectively permit or deny packets on a port based on whether a packet is associated with certain predefined MAC addresses. A MAC address filter is typically used to control the inbound flow of traffic only. In accordance with an embodiment of the present invention,



one MAC address filter can be configured per port in the inbound direction and no MAC address filter is configured in the outbound direction. However, the invention is not so limited and, in an alternate embodiment, multiple MAC address filters can be configured per port in the inbound direction and one or more MAC address filters can be configured per port in the outbound direction.

**[0059]** FIG. 5 illustrates a flowchart 500 of a method for performing user authentication and dynamic user policy assignment in accordance with an embodiment of the present invention. The invention, however, is not limited to the description provided by the flowchart 500. Rather, it will be apparent to persons skilled in the relevant art(s) from the teachings provided herein that other functional flows are within the scope and spirit of the present invention. Flowchart 500 will be described with continued reference to example system 100 described above in reference to FIG. 1. The invention, however, is not limited to that embodiment.

**[0060]** The method of flowchart 500 begins at step 502, in which user device 108 attempts to access data communications network 104 via network access device 102. In response, network access device 102 places 802.1x client software on user device 108 into an unauthorized state that permits the client software to send only an EAP start message, as shown at step 504. Network access device 102 also returns an EAP message to user device 108 requesting the identity of the user, as shown at step 506.

**[0061]** At step 508, the user of user device 108 inputs identity information or credentials, such as a user name and password, into user device 108 that are returned to network access device 102. Network access device 102 then generates an authentication call which forwards the user credentials to authentication server 106, as shown at step 510, and authentication server 106 performs an algorithm to authenticate the user based on the user credentials, as shown at step 512.

**[0062]** At step 514, authentication server 106 returns either an accept or reject message back to network access device 102. As shown at step 516, if

authentication server 106 sends a reject message back to network access device 102, the protocol proceeds to step 518. At step 518, network access device 102 blocks all traffic on the port except for the reception or transmission of 802.1x control packets (e.g., EAPOL packets) on the port. However, if authentication server 106 sends an accept message back to network access device 102, then the protocol proceeds to step 520.

**[0063]** At step 520, network access device 102 parses the accept message to determine if user policy has been provided for the user. In an embodiment of the present invention, authentication server 106 provides a user policy by populating a Filter-ID and/or a Vendor-Specific Attributes fields of a RADIUS Access-Accept message. The format of an Access-Accept message and the individual fields included therein is described in IETF RFC 2865 and RFC 2138, the contents of which are incorporated by reference as if set forth fully herein.

**[0064]** In an embodiment, the Filter-ID field is used to identify one or more Access Control Lists (ACLs) or MAC address filters that are already configured on network access device 102. A name or number may be used to identify a configured ACL. For example, text formatted as follows may be included in the Filter-ID to specify a configured standard or extended IP ACL in either the inbound or outbound direction:

Numbered IP ACL inbound direction:      ip.number.in

Named IP ACL inbound direction:          ip.name.in

Furthermore, text formatted as follows may be included in the Filter-ID to specify a configured MAC address filter in the inbound direction:

Numbered MAC Address Filter inbound direction: mac.number.in

**[0065]** In an embodiment, the Vendor-Specific Attributes field is used to provide one or more actual ACLs or MAC address filters for dynamic

configuration by network access device 102. For example, text formatted as follows may be included in the Vendor-Specific Attributes field to pass a standard or extended IP ACL to network access device 102:

Named Standard IP ACL inbound direction:	ipacl.s.in=<entry>
Named Standard IP ACL outbound direction:	ipacl.s.out=<entry>
Named Extended IP ACL inbound direction:	ipacl.e.in=<entry>
Named Extended IP ACL outbound direction:	ipacl.e.out=<entry>

Furthermore, text formatted as follows may be included in the Vendor Specific Attributes field to pass a MAC address filter

MAC address filter inbound direction:	macfilter.in=<entry>
---------------------------------------	----------------------

[0066] As shown at step 522, if a user policy has not been provided as part of the accept message, then network access device 102 does not assign a user policy to the port. However, if a user policy has been provided as part of the accept message, then network access device 102 determines if the user policy is valid, as shown at step 524. For example, if the user policy identifies a configured IP ACL and/or MAC address filter, then network access device 102 will confirm that it supports such an IP ACL and/or MAC address filter. Alternately, if the user policy actually includes an IP ACL and/or MAC address filter, network access device 102 will determine whether the IP ACL and/or MAC address filter has been provided in a valid format for dynamic assignment to the port.

[0067] If the user policy provided as part of the accept message is not valid, then network access device 102 blocks all traffic on the port except for the reception or transmission of 802.1x control packets (e.g., EAPOL packets) on the port, as shown at step 526. However, if the user policy is valid, then network access device 102 determines whether sufficient system resources are available to dynamically assign the user policy to the port, as shown at step

528. If sufficient resources are not available, then network access device 102 blocks all traffic on the port except for the reception or transmission of 802.1x control packets (e.g., EAPOL packets) on the port as shown at step 530. However, if there are sufficient resources available, then network access device 102 dynamically assigns the user policy to the port and then restricts further traffic on the port in accordance with the policy, as shown at step 532.

[0068] In accordance with an embodiment of the present invention, ACLs that are already configured on network access device 102 and ACLs that are received for dynamic port assignment are identified by numbers from different number ranges, thereby allowing network access device 102 to distinguish between the two types of ACLs. Network access device 102 can use this information to ensure, for example, that an ACL received for dynamic assignment is not automatically saved when a “write memory” function is executed to save configuration information to a start-up configuration file. By using a different numbering range, network access device 102 can easily determine if there are any dynamic ACLs configured on the device and execute the “write memory” feature appropriately. Alternatively, network access device 102 can warn an administrator that a dynamic user policy has been configured and allow them to either save it or not save it when they perform a “write memory.”

[0069] In accordance with a further embodiment of the present invention, the above-described method for dynamic user policy assignment is implemented in combination with a method for dynamic VLAN assignment as described in co-pending and co-owned U.S. Patent Application Serial No. 10/458,628, entitled “Multiple Tiered Network Security System and Apparatus” to Kwan *et al.*, filed June 11, 2003, the entirety of which is incorporated by reference as if set forth fully herein. In accordance with such a combination, the accept message received from authentication server 106 may also include a VLAN identifier that permits network access device 102 to dynamically assign the port to a VLAN associated with the user. The combination of dynamic user

policy assignment and dynamic VLAN assignment can provide an even greater level of network access control if so desired.

E. Multiple Tiered Security System, Method and Apparatus for Multi-Host Environments in Accordance with an Embodiment of the Present Invention

[0070] The multiple tiered security protocol described above may be advantageously implemented in both single host and multiple host (multi-host) environments. FIG. 1 depicts a single host environment, as only a single user device 108 is coupled to a port of network access device 102. FIG. 6 depicts an alternate embodiment of the present invention that accommodates a plurality of user devices in a multi-host configuration. In particular, FIG. 6 a multiple tiered network security system 600 that comprises a data communications network 104, a network access device 602 and an authentication server 106 each of which is communicatively coupled to data communications network 104. A central user device 604 is coupled to network access device 602 and a plurality of additional user devices 606a through 606n are coupled to network access device 602 via central user device 604 in a multi-host configuration.

[0071] The multiple tiered security protocol described above may be advantageously implemented in system 600 in a variety of ways. For example, network access device 602 may perform physical (MAC) address authentication of central user device 604 only, and then authenticate the users of all the user devices if it determines that central user device 604 has a valid MAC address. If central user device 604 has an invalid MAC address, then the port may be closed to all user devices. Alternately, network access device 602 may perform physical (MAC) address validation of each of the user devices prior to authenticating their users. In this case, network access device 602 can selectively accept packets from user devices having valid MAC addresses while dropping packets from user devices having invalid MAC addresses.

F. Conclusion

[0072] While various embodiments of the present invention have been described above, it should be understood that they have been presented by way of example only, and not limitation. It will be understood by those skilled in the relevant art(s) that various changes in form and details may be made therein without departing from the spirit and scope of the invention as defined in the appended claims. Accordingly, the breadth and scope of the present invention should not be limited by any of the above-described exemplary embodiments, but should be defined only in accordance with the following claims and their equivalents.